

Hurricane Katrina Update *New* Direction

Inside This Issue

This is a Newsletter of the SPAWAR Systems Center New Orleans

**Task Force Navy Family
Leaders Visit SSC NOLA**

**Safeguard Your Identity this
Holiday Season**

**Janet Knauer: SPAWARRIOR of
the Quarter**

Holiday Guidance

**Safety Tip: Emergency Notifica-
tion Cards**

**Important Numbers and Web
Sites**

DIMHRS and NSIPS Ready to Return to the Big Easy

By Teresa Leger
SSC NOLA Public Affairs Office

With the imminent arrival of Hurricane Katrina, not only did SSC New Orleans prepare to relocate, but two of our biggest customers, the Defense Integrated Military Human Resources System (DIMHRS) Joint Program Management Office (JPMO) and the Navy Standard Integrated Personnel System (NSIPS) who share our lakefront facilities also implemented their Continuity of Operations Plans (COOPs).

As with most New Orleanians, both DIMHRS and NSIPS thought it would be a temporary relocation. However, after the realization that this was not like any other activation of their COOP plans, they immediately made arrangements to relocate personnel and continue operations elsewhere.

DIMHRS has continued their operations out of three locations within the

Washington DC area. They were up and running immediately after Labor Day. NSIPS temporarily relocated to the Naval Support Activity (NSA) Mid-South in Millington, Tennessee.

Over 225 government and contractor personnel are still working on the DIMHRS project from the Washington DC area while approximately 40 personnel are working from offices in Pensacola, Florida; Slidell, and Mandeville. Some have also begun telecommuting from their residences in and around the New Orleans area while others alternate from telecommuting to working out of the offices in the DC area.

The NSIPS production operations were moved from the SSC New Orleans facilities to Millington with no impact to the active duty users and only minimal impact to the reserve users on the weekend before Hurricane Katrina hit.

[Continued](#)

If you have information or photos you'd like to submit for consideration in the newsletter please send to maria.tolleson@navy.mil or mstolleson@yahoo.com

Janet Knauer: SPAWARRIOR of the Quarter

By Maria LoVasco Tolleson
SSC NOLA Public Affairs Officer

Janet Knauer, Engineering Process Division, was named SPAWARRIOR of the Quarter for the first quarter of the calendar year for the entire SPAWAR Command.

RADM (sel) Tim Flynn, SPAWAR Vice Commander, presented the plaque to her in the hallowed out Operations Deck of Building 3 before a gathering of SSC New Orleans leaders and technical employees during a recent visit. Flynn is a native of New Orleans and attended Jesuit High School. He still has family in the area who were also affected by the storm.

Knauer was recognized for her significant contribution to the redesign, deployment, and maintenance of the SSC New Orleans Process Library, the Project Repository, the Check-in/Check-out database, process deployments, and other Engineering Process Division initiatives.

"As a junior employee you consistently perform at an exceptional level well beyond the required standards and have established yourself as a very dependable, self-motivated, and highly productive individual that goes the extra mile to produce high quality results," Flynn said.

Flynn stated that Knauer exemplified the great workforce of the SSC New Orleans. During his congratulatory remarks he praised the SSC New Orleans employees for their efforts in relocating servers and equipment to alternate work sites in the days immediately after the hurricane to continue to support the Navy's pay and personnel systems.

"I have heard of your heroic efforts in the aftermath of one of the most cataclysmic events to hit the U.S.," he said. "That you were doing this while your own homes were destroyed, and your own families were displaced is quite an accomplishment. No one expected you to keep doing your job in the face of such challenging difficulties, but you didn't miss a beat. My hat is off to you."

Knauer recently completed the final phase of the three-tiered Lean Six Sigma (LSS) Black Belt Training. She is now certified as an LSS Black Belt.



RADM (sel) Tim Flynn, SPAWAR Vice Commander, presents Janet Knauer with the SPAWARRIOR of the Quarter plaque.

Important Numbers and Web Sites

- q Navy Global Distance Support Center (to update your location and contact information), 1-877-418-6824, Option 2 or www.anchordesk.navy.mil
- q BUPERS 24-hour Helpline, 1-877-414-5358
- q Safe Haven Orders, 1-866-239-0303
- q 24-hour Support Hotline, 1-800-677-5327
- q SSC NOLA Executive Officer, 1-850-452-5810
- q Per Diem Rates <https://secureapp2.hqda.pentagon.mil/perdiem/perdiemrates.html>
- q FEMA, 1-800-621-3362 or www.fema.gov
- q Red Cross, www.redcross.org
- q DOD Civilian Personnel Management Service: Hurricane Information for DOD Civilian Employees and Annuitants, <http://www.cpms.osd.mil/hurricaneinfo/index.htm>
- q Civilian Employee Assistance Program, 1-800-677-LEAP
- q Federal Tax Relief, www.irs.gov, select "help for hurricane victims"

This is a publication produced by the Space and Naval Warfare Systems Command (SPAWAR) Systems Center New Orleans' Public Affairs Office located at 2251 Lakeshore Drive, New Orleans, LA 70145. The content of this publication does not reflect the views, opinions, or policies of the Department of the Navy or the Department of Defense.

Task Force Navy Family Leaders Visit New Orleans

By Maria LoVasco Tolleson
SSC NOLA Public Affairs Officer

RADM Robert O. Passmore, Commander, Task Force Navy Family and RADM Donald R. Gintzig, Deputy Commander, Task Force Navy Family were in the New Orleans area this week to visit local Navy commands and to thank the Naval Air Station (NAS) New Orleans Navy Band for a series of morale boosting concerts given along the devastated Gulf Coast. While in New Orleans, they visited the Naval Support Activity in Algiers, the Fleet Family Support Center at NSA New Orleans, the NAS Joint Reserve Base (NAS JRB) in Belle Chasse, and the Community Support Center at NAS JRB.

Before departing back to Washington, D.C., they made one final stop to SSC New Orleans to look at the facility and speak to the command's leadership. Accompanying Passmore was his wife, a volunteer Ombudsman at Large with Task Force Navy Families. Passmore is also the Vice Commander, Naval Reserve Forces Command Deputy Commander, Navy Region Northwest. Gintzig is also the Associate Chief, Bureau of Medicine and Surgery, Health Care Operations and the Deputy Director for Reserve Affairs, Medical Service Corps.

The mission of Task Force Navy Family is to coordinate full spectrum community service operations to provide a rapid return to a stable environment for all affected Navy families. Full-spectrum community service operations include but are not limited to:

- * Full accounting of affected Navy Families
- * Temporary Housing for Navy Families, as authorized
- * Way ahead for permanent housing for Navy Family
- * Financial assistance and counseling, as desired

RADM (right) Robert O. Passmore, Commander, Task Force Navy Family and RADM Donald R. Gintzig, Deputy Commander, Task Force Navy Family (left) visited the SSC New Orleans facility during a trip to Navy commands along the affected Gulf Coast.



- * School children of affected Navy Families return to school
- * Transportation options for relocation, return to work and school, where possible
- * Access to health care services
- * Access to counseling / pastoral care
- * Access to child care
- * Access to legal services (including claims support)
- * Employment support for family / civilians
- * Pay and benefits

For more information on Task Force Navy Family go to:
<http://taskforcenavyfamily.navy.mil/NavyFamilies/>.

Safeguard Your Identity this Holiday Season

By Ernest Mitchell
SSC NOLA Operations Security Officer

As the holiday season approaches, many personnel will find themselves shopping online for that perfect gift. However, the reality is that Identity Theft is still an every growing problem.

To help you protect yourself, below is some information to assist you in protecting personal information when receiving suspicious emails and requests—even from what appear to be legitimate sites and requests.

Phishing and Pharming are two words which all internet users should be familiar with in today's society.

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials.

Social engineering schemes use 'spoofed' or forged e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords, and social security numbers. By hijacking brand names of banks, e-retailers, and credit card companies, phishers often convince recipients to respond to the e-mail inquiries.

Technical subterfuge schemes plant crimeware onto personal computers (PCs) to steal credentials directly, often using Trojan keylogger spyware.

Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS (Data Source Name) hijacking or poisoning.

The Anti-Phishing Working Group website, <http://www.antiphishing.org>, can provide additional information on Phishing and http://www.antiphishing.org/phishing_archive.html can provide examples of phishing attacks. Consumer Advice on how to avoid Phishing Scams

can be found at http://www.antiphishing.org/consumer_rec.html.

Online banking is becoming as common as direct deposits. While online banking and e-commerce is very safe, as a general rule you should be careful about giving out your personal financial information over the Internet. The Anti-Phishing Working Group has compiled some recommendations you can use to avoid becoming a victim of these scams.

First, be suspicious of any email with urgent requests for personal financial information. Unless the email is digitally signed, you can't be sure it wasn't forged or 'spoofed'. Phishers typically include upsetting or exciting (but false) statements in their emails to get people to react immediately. They typically ask for information such as usernames, passwords, credit card numbers, or social security numbers. Emails from Phisher are usually not personalized, while valid messages from your bank or e-commerce company generally are.

Also, don't use the links in an email to get to any web page even if you suspect the message might be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the web address in your browser.

Avoid filling out forms in email messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone.

Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browsers address bar - it should be "https://" rather than just "http://."

[Continued](#)

Safeguard Your Identity (continued)

Consider installing a web browser tool bar to help protect you from known phishing fraud websites. EarthLink ScamBlocker is part of a free browser toolbar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phisher web sites. It's free to all Internet users and can be download at <http://www.earthlink.net/earthlinktoolbar>.

You should also regularly log into your online accounts. Don't wait for a month before you check each account. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate.

If you find anything suspicious, contact your bank and all card issuers immediately and ensure that your browser is up to date and security patches applied.

For those who use the Microsoft Internet Explorer browser, immediately go to the Microsoft Security home page (<http://www.microsoft.com/security/>) and download a special patch relating to certain phishing schemes.

If you are a victim of "phishing" or a "spoofed" e-mail, you should forward the e-mail to reportphishing@antiphishing.com, to the Federal Trade Commission at spam@uce.gov, and to the "abuse" email address at the company that is being spoofed (for example "spoof@ebay.com").

When forwarding spoofed messages, always include the entire original email with its original header information intact and notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov/.

DIMHRS & NSIPS (continued)

Initially, NSIPS personnel evacuated to various locations, but now all but three are working in Millington where they share working space with the NMCI operations personnel responsible for the NSIPS COOP environment. "Captain Matt Straughan, the Commanding Officer for NSA Mid-South and his staff have been very helpful," said CDR Susan Eaton, NSIPS Program Manager. "Pat Huiatt the SSC NOLA rep in Millington has also been tremendously helpful."

Two of the other three NSIPS staff have returned to the New Orleans area where they are working out of the Dauphine Street facilities and one is working with CDR Eaton in Virginia.

Although, both NSIPS and DIMHRS lost some personnel due to the tragedy of Katrina and the impact it had on their families and personal lives, most of their government and contractor personnel have continued to work at temporary locations.

"The Program is committed to re-turning folks to the New Orleans area as quickly as possible," said Jenna Noble, Acting Joint Program Manager, DIMHRS (Pers/Pay). "Once the SSC New Orleans facilities are available and personnel are able to find suitable housing arrangements, the DIMHRS JPMO plans to return to New Orleans."

NSIPS has also stated that they too plan to return personnel to New Orleans. "We're already planning our return and will do so when SSC NOLA and the city infrastructure are habitable and can support us back there," said Eaton.

Both programs are pleased with the service and work they have been able to continue to perform with the hard work and dedication of their staff. However, they are eager to return to Louisiana and the beautiful facilities at the lakefront.

***Safety Tip:* Emergency Notification Cards**

Many personnel have been displaced from their homes and are living with relatives or friends or find themselves in apartments or temporary housing. Therefore, the address on your driver's license may not be the location where you are currently living. In case of an accident or emergency situation, you may wish to place an additional emergency notification card in your wallet or purse near where you keep your drivers license. The card should include your current address, contact information, an emergency contact which includes cell phone numbers as well as information regarding any medical condition or medication you are currently taking.

Holiday Guidance

The holiday season traditionally involves parties, receptions, and exchanging gifts. However, even during the holiday season, the Standards of Conduct must apply. To ensure you don't unwittingly violate the standards, information on the rules regarding receptions, parties, and gift exchanges which involve co-workers, contractors, and supervisors is outlined below.

Gifts from Contractors:

Federal personnel may not accept gifts offered because of their official positions or offered by a "prohibited source." A prohibited source is anyone who seeks official action by the employee's agency; anyone who does business or seeks to do business with the employee's agency; anyone who conducts activities regulated by the employee's agency; anyone who has interests that may be substantially affected by the employee's performance of duty, or any organization composed of members who are described above.

The general rule is that federal personnel may not accept gifts from prohibited sources, including contractors and contractor personnel. However, there are a few exceptions. A gift that does not exceed a \$20 value and is not cash may be accepted as long as the total amount of gifts that the person accepts from that source does not exceed \$50 for the year. A gift based on a bona fide personal relationship such as personal gifts that are actually paid for by the contractor employee rather than the contractor can be accepted.

Many contractors have rules of ethics

or business practices that are similar to the Federal rules. Take these rules into consideration before offering contractor employees gifts or opportunities that they may not be able to accept.

Receptions or Open-houses with Contractors:

Generally, federal personnel can attend an open-house or reception and accept any gift of refreshments if it is a widely attended gathering and the employee's supervisor determines that it is in the agency's interest that the employee attends. Social events sponsored by non-prohibited sources may be attended by federal personnel as long as there is no charge for admissions.

Invitations that are open to the public, open to all government employees, or open to all military personnel can be accepted by federal personnel even if the invitation comes from a contractor.

Federal personnel can accept invitations offered to a group or class that is not related to government employment. For example, if the building owner where the office spaces are located throws a reception for all of the tenants of the building, government personnel may attend.

Refreshments consisting of soft drinks, coffee, pastries, or similar refreshments not constituting a meal may be accepted since they are not considered to be a gift.

If there is an outside business or relationship that requests attendance at an event such as a spouse working for a contractor, a federal employee may accompany the spouse since the invitation is to the spouse and not the federal employee.

Gift or Parties Involving Supervisors and Co-workers:

Supervisors may accept personal hospitality at the residence of a subordinate that is customarily provided on the occasion and there are no restrictions on a subordinate accepting an invitation from a boss or co-worker.

As a general rule, federal supervisors may not accept gifts from subordinates or federal personnel who receive less pay than them. However, during the holidays, which occur on an occasional basis, supervisors may accept gifts from subordinates other than cash valuing \$10 or less. Supervisors may also accept food and refreshments shared in the office and may share in the expenses of an office party. If a subordinate is invited to a social event at the supervisor's residence, the subordinate may give the supervisor a hospitality gift of the type and value customarily given on such an occasion.

There are no legal restrictions on gifts given to peers or subordinates, however, common sense and good taste should apply.

Outside solicitation of contributions towards a party is not acceptable. This includes the solicitation of funds, food or any items. Generally office parties are unofficial events and appropriated funds may not be used to pay for them.

This guidance only highlights common questions, and does not cover every situation. If you are unsure, contact either John Higley or Rich Walls, Ethics Counselors, in the SPAWAR Office of Counsel, Code 00C-3, OT-4, Rm 1118, 619-524-7042 or 619-524-7045.